

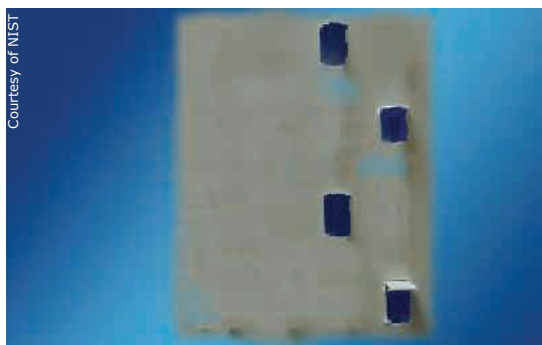
Every Vote Counts...Or Does It?

Is electronic voting the right way to go?

by Niran Babalola

On the night of November 7, 2000, millions of Americans sat in front of their televisions waiting for the result of the day's presidential election. No one predicted it would be another full month until any conclusion was reached. As a result of the month of uncertainty and the many months of litigation that followed, citizens and their Congressional representatives demanded a way to ensure that this mess of a voting process would never happen again. In October 2002, Congress passed the Help America Vote Act (HAVA) to "establish a program to provide funds to states to replace punch card voting systems" and to generally improve the national voting process by January 2006. Currently, the most popular replacements for antiquated voting methods are electronic voting machines equipped with touch screens. Most of these devices are Direct Recording Electronic (DRE) machines, which record entered votes inside the computer and print out the results at the end of the election. Though skeptics are wary of its pitfalls, dissatisfaction with the old voting system has pushed more and more people to look towards electronic voting as a viable alternative.

These machines, manufactured by companies such as Diebold and Sequoia, have been hailed as the solution to many of the problems presented by paper voting. Though there has been hours of news coverage given to the infamous "hanging chad" of the Florida 2000 recount, ambiguity of voter intention is just one of the many difficulties in the traditional electoral process. Another problem that is often ignored is the accommodation of voters with disabilities such as severe visual impairment. Traditionally, it was



Hanging chads, a major part of the 2000 election controversy, would be eliminated with e-voting.

very difficult to cast your vote if you could not see the choices on the ballot but the new computerized voting systems comes equipped with a audio devices that can potentially make voting as easy as plugging in headphones and pressing a button. Electronic voting machines were used widely in the Super

Tuesday primaries on March 2, 2004. Some visually impaired voters who used the machines referred to the experience as "the easiest vote [they] have ever had," according to the Baltimore Sun.



Direct Recording Electronic (DRE) machines could allow citizens to cast their vote electronically.

Although these machines seem like an elegant solution to the issues at hand, their introduction has raised an alarm among computer scientists around the nation who worry about their reliability. Afterall, with an electronic voting system a recount to double check the results of the system would be meaningless because the computers would merely regurgitate the same results over and over. In an attempt to resolve this issue, David Dill, a Computer Science professor at Stanford, has taken matters into his own hands by helping to create an organization called VerifiedVoting.org in an effort to obtain "transparent, reliable, and publicly verifiable elections in the United States." He cites the lack of a voter-verifiable paper trail, or a paper copy of each vote, as the main flaw with DRE voting machines. Currently, these machines allow the voter to enter his or her choices and then save this information in a database. Ultimately, however, the voter has no way of knowing if the computer has recorded his or her vote as it was meant to be entered. In other words, there is no reliable way to check if an error has been made.

Professor Dill's solution to this dilemma is basically two simultaneous elections: one which occurs inside the computer and another that uses ballots that would be printed out by the machine and verified by the voter as showing the result that was intended. The latter of these would only be used during a recount. Providing a publicly-verifiable paper trail would allow election officials to use the paper record of the votes to check if the machines made a mistake.

Another danger of the transition from paper to electronic voting is the ease of fraud. Swaying an electronic election is as easy as inserting a few lines of cleverly hidden code into the program that could easily go undetected throughout the election. To alter a paper



election, on the other hand, would be more likely to require the collaboration of a large group who would have to go through the much more difficult process of forging votes in multiple locations across the domain of the election. Dill believes that with electronic voting, “somebody can change those lines of code before the software is installed on the machines. One person can change the software and then the change could go into thousands and thousands of machines across the country, whereupon lots and lots of votes could be changed.”

Companies who make electronic voting machines rebut this criticism by claiming that their devices are put through rigorous testing to ensure that no bugs or security flaws are present in the machines. In addition, they are tested by independent agencies in order to obtain state certification to be used in elections. Unfortunately, if a bug or malicious code makes it past these barriers, there is no way for anyone to know of the problem without a voter-verifiable paper trail. To address this issue, a group of computer scientists have formed the Open Voting Consortium, a non-profit organization that seeks to produce an open source electronic voting alternative where the programming code used to design the machines would be widely available. VoteHere, a commercial electronic voting machine company, has followed suit, making their source code available to download on their website. This initiative would allow anyone to inspect the instructions running the software behind the scenes. The reasoning behind this approach is that the more eyes that examine the source code, the more confident the public can be that no malicious information lurks in the software.

Even with a thorough examination of source code, performing a recount is the only way to be sure the machines are working as expected and the only way to get a meaningful recount is to have a voter-verifiable paper trail. Professor Dill and his organization have been at the forefront of the movement to use the

joint electronic-paper system. Congressman Rush Holt of New Jersey introduced the Voter Confidence and Increased Accessibility Act in March of 2003. If passed, this bill would require all voting machines to have a verifiable paper trail by the November 2004 election. Precincts that do not meet the requirement would continue using the paper systems. Surprise recounts would be performed in 0.5% of jurisdictions using the paper printouts to ensure that no errors are present in the software.

The bill and its counterpart in the Senate are facing stiff resistance from those who believe a paper trail would infringe on voters’ right to privacy. For example, critics claim that in the case of a paper jam with the printer, whoever clears it will see the vote that jammed the machine. Defenders argue that since printers are used constantly in ATM’s, stores and various other places while jamming infrequently there is no reason this application would be any more error prone. Dill estimates that a jam might occur at “once in every few polling places,” and even so, the printers could be constructed so that clearing a jam would not require seeing the printed vote. In considering these possibilities, the system can be designed to uphold voters’ right to privacy while obtaining clear confirmation of the voting decision. Without a voter-verifiable paper trail, there is no way for a voter to be sure that their vote is being counted when using an electronic voting machine.

Critics of the new electronic voting systems are playing an important role in the debate by bringing to light the possible loopholes of the new system. As a result, we can initiate new measures to increase the reliability and accuracy of electronic voting. Currently, it looks like the relative ease and lack of ambiguity of an electronic vote are likely to make it a part of our future. If, however, anyone feels strongly against the electronic system voting on paper is always “a way of recording a protest vote against the DRE’s,” says Dill. Ultimately, though, “the most important thing is to vote. If your only choice, or your only convenient choice, is to vote on a [DRE], I would encourage people to hold their noses and do it and vote for politicians who will get rid of the [DRE’s].” **S**

Editor’s Postscript:

As the November 2004 elections fast approach, pressure is mounting for states to be ready when the public goes to the polls. Several weeks after this article was written, on April 30, 2004, California Secretary of State, Kevin Shelley banned the use of touchscreen, electronic voting systems until security measures are put in place to ensure their reliability. In Shelley’s eyes, as in Professor David Dill’s, the fundamental problem with the system is the lack of a voter verifiable paper-trail. Though this is a blow for electronic voting proponents in the short-run, stringent security measures will hopefully lead to a better system once touchscreen voting systems become the norm.

Courtesy of <http://www.ss.ca.gov>



California is one of many states which has already adopted DRE machines in some precincts.